

Vysoká škola báňská – Technická univerzita Ostrava

Fakulta strojní

Katedra automatizační techniky a řízení

Studijní opory pro praktickou výuku WiFi technologií  
v týmech

Educational Support for Practical Training Of WiFi  
Technology Of Student's Teams

Vedoucí bakalářské práce:

Ing. David Fojtík, Ph.D.

Student:

Jan Kvapil

Ostrava 2012

## Zadání bakalářské práce

Student: **Jan Kvapil**  
Studijní program: B2341 Strojírenství  
Studijní obor: 3902R001 Aplikovaná informatika a řízení  
Téma: Studijní opory pro praktickou výuku WiFi technologií v týmech  
Educational Support for Practical Training of WiFi Technology of  
Student's Teams

Zásady pro vypracování:

1. Popište technologii WiFi a její standardy.
2. Seznamte se s problematikou týmové práce a navrhněte změnu koncepce předmětu Management počítačových sítí s cílem inovovat cvičení o praktickou výuku WiFi technologií v týmech.
3. Navrhněte sadu týmových úkolů zaměřených na výuku WiFi technologií a zpracujte návody ke cvičení.
4. Zhodnoťte dosažené výsledky a navrhněte směry dalšího řešení.

Seznam doporučené odborné literatury:

FARANA, R., SMUTNÝ, L., VÍTEČEK, A., VÍTEČKOVÁ, M., WAGNEROVÁ, R. *Doporučení pro psaní odborných textů z oblasti automatizace a informatiky*. Skripta FS VŠB-TU Ostrava, 2008, 80 str. ISBN 978 - 80 - 248 - 1925 - 9  
KÖHRE, T. *Stavíme si bezdrátovou síť Wi-Fi*, Praha: Computer Press 2004. 296 s. ISBN: 80-251-0391-9  
PAYNE, V. *Teambuilding workshop - Trénink týmových dovedností*. 1. vyd. Praha: Computer Press 2007. 339 s. ISBN: 978-80-251-1588-6  
PECHAČ, P. *Šíření vln v zástavbě*. Praha: BEN - technická literatura 1. vyd. 2005. 108 s. ISBN 80-7300-186-1  
PUŽMANOVÁ, R. *Bezpečnost bezdrátové komunikace*. 1. vyd. Brno: Computer press, 2005. 179 s. ISBN 80-251-0791-4.  
ZANDL, P. *Bezdrátové sítě WiFi – Praktický průvodce*. 1. vyd. Brno: Computer press, 2003. 190 s. ISBN 80-7226-632-2.

Formální náležitosti a rozsah bakalářské práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí bakalářské práce: **Ing. David Fojtík, Ph.D.**

Datum zadání: 16.12.2011

Datum odevzdání: 21.05.2012



prof. Ing. Jiří Tůma, CSc.  
vedoucí katedry



prof. Ing. Radim Farana, CSc.  
děkan fakulty

**Prohlášení studenta**

Prohlašuji, že jsem celou bakalářskou práci včetně příloh vypracoval samostatně pod vedením vedoucí bakalářské práce a uvedl jsem všechny použité podklady a literaturu.

**V Ostravě 13. 5. 2012**

**podpis studenta .....**

**Prohlašuji, že**

- jsem byl seznámen s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. – autorský zákon, zejména §35 – užití díla v rámci občanských a náboženských obřadů, v rámci školních představení a užití díla školního a §60– školní dílo.
- беру на вѣдомі, že Vysoká škola báňská – Technická univerzita Ostrava (dále jen VŠB-TUO) má právo výdělečně ke své vnitřní potřebě bakalářskou práci užít (§35 odst. 3).
- souhlasím s tím, že jeden výtisk bakalářské práce bude uložen v Ústřední knihovně VŠB-TUO k prezenčnímu nahlédnutí a jeden výtisk bude uložen u vedoucího bakalářské práce. Souhlasím s tím, že údaje o bakalářské práci budou zveřejněny v informačním systému VŠB-TUO.
- bylo sjednáno, že s VŠB-TUO, v případě zájmu z její strany, uzavřu licenční smlouvu s oprávněním užít dílo v rozsahu §12 odst. 4 autorského zákona.
- bylo sjednáno, že užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití mohu jen se souhlasem VŠB-TUO, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly VŠB-TUO na vytvoření díla vynaloženy (až do jejich skutečné výše).
- беру на вѣдомі, že odevzdáním své práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, bez ohledu na výsledek její obhajoby.

V Ostravě 21. 5. 2012

podpis studenta.....

Adresa trvalého pobytu:

Jiříkov 98

Jiříkov

PSČ: 79351

## **Anotace**

KVAPIL, J. Studijní opory pro praktickou výuku WiFi technologií v týmech: Bakalářská práce. Ostrava: VŠB – Technická univerzita Ostrava, Fakulta strojní, Katedra automatizační techniky a řízení, 2012. 57 s. Vedoucí práce Fojtík, D.

Bakalářská práce se zabývá výukou specifických okruhů technologie WiFi formou týmových úloh. Hlavním výstupem je studijní opora, která prostřednictvím připravených praktických úloh určených pro studentské týmy, seznamuje studenty s danou technologií a problematikou týmové práce.

## **Annotation**

KVAPIL, J. Study support for the practical work with WiFi technology in teams: Bachelor work. Ostrava: VSB – Technical University Ostrava, Faculty of Mechanical Engineering, Department of Control Systems and Instrumentation, 2012. 57 s. Thesis head Fojtík, D.

This Bachelor thesis deals with the teaching of typical areas of WiFi technology by way of team tasks. The main output of this thesis is the study support, which by way of practical tasks designed for student teams, familiarizes students with the technology and problems solving in teamwork.

# Obsah

1	Bezdrátové sítě.....	10
1.1	Standardy WIFI sítí.....	10
1.2	Antény, přijímače.....	15
1.2.1	Typy antén pro bezdrátové sítě sítí .....	15
1.2.2	Technické parametry antén.....	18
1.2.3	Polarizace antén .....	19
1.3	Konektory a kabely .....	21
1.3.1	Kabeláž .....	21
1.3.2	Náhrada koaxiálního kabelu.....	22
1.3.3	Konektory.....	23
1.4	Další hardware pro bezdrátové sítě.....	23
1.4.1	Access Point (Bezdrátový přístupový bod) .....	23
1.4.2	Router.....	24
1.4.3	Wireless Bridge.....	24
2	Problematika týmové práce .....	26
2.1	Pravidla dobrého týmového rozhodování .....	27
2.2	Základní typy rolí.....	27
2.3	Typy týmových rolí .....	28
3	Předmět Management počítačových sítí .....	30
4	Návrh týmových úloh pro předmět Management počítačových sítí .....	32
4.1	Úloha: Správné umístění antény přístroje v prostorách bytu.....	32
4.2	Úloha: Vytvoření firemní sítě .....	35
4.3	Úloha: Zabezpečení a prolomení bezdrátové sítě .....	36
5	Realizace zadaných úloh.....	38
5.1	Realizace zabezpečení a prolomení bezdrátové sítě .....	38
5.2	Realizace úlohy vytvoření firemní sítě .....	43
5.3	Realizace správného umístění antény přístroje v prostorách bytu.....	50
6	Závěr .....	53
7	Seznam použité literatury .....	55

## Seznam použitých zkratk a pojmů

WiFi	Wireless Fidelity = Komunikační standard pro bezdrátový přenos dat
XML	Xtensible Markup Language = Rozšiřitelný značkovací jazyk
ISM	Industrial Scientific and Medical=Rádiové frekvence přiděleny pro průmyslové, vědecké a lékařské procesy
GSM	Global Systemfor Mobile Communication = Globální systém pro mobilní komunikaci
CDMA	Code Division Multiple Access =Kódové dělení přenosových kanálů
UMTS	Universal Mobile Telecommunication Systém = Univerzální mobilní telekomunikační systém
FWA	Fixed Wireless Access = Síť pevného bezdrátového přístupu
FCC	Federal Communications Commission = Federální komunikační komise
ETS	European Technical Standarts Institute = Evropský institut pro technické standardy
IEEE	Institute of Electrical and ElectronicsEngineers = Společnost pracovníků v elektrotechnice a elektronice v USA
BSS	Basic Service Set = Základní sada služeb
MAC	media accesscontro = Řízení přístupu k médiím
ISO	International Organization for Standardization = Mezinárodní organizace pro normalizaci
WEP	Wireline Equivalent Privacy = Pevné ekvivalentní soukromí
OFDM	Orthogonal Frequency Division Multiplexing= Ortogonální multiplex s kmitočtovým dělením
PDA	Personal Digital Assistant = Kapesní počítač

Ping            Packet Inter Net Groper = Umožňuje prověřit funkčnost spojení mezi dvěma  
síťovými rozhraními



# Úvod

Stejně jako mobilní telefony se postupem času mění, mění se i společenské zvyklosti, které přinesly změnu i do počítačového světa. Ještě před několika desítkami let se považovalo propojení počítačů mezi sebou za něco nepředstavitelného. Ale není tomu tak dlouho, co se celosvětová počítačová síť Internet stala součástí našich životů, a málokterý člověk by si dokázal představit život bez této dominanty dnešní doby. Dnes již víme, že počítač nemusí být striktně upoután na jednom místě, aby mohl tuto síť plnohodnotně využívat.

WiFi sítě jsou v dnešní době velmi používanou technologií nejen pro svou praktičnost, ale i pro svou pohodlnost. Práce se zabývá problematikou této technologie od budování bezdrátových sítí, až po ochranu a zabezpečení dat proudících po sítích WiFi. Dále se práce zabývá rekonstrukcí předmětu Management počítačových sítí, obsahuje tedy i informace o něm. Účelem předmětu je dopracovat se od praktických pokusů k základům teorie. Studenti dostanou za úkol vypracovat různé úlohy, tyto úlohy mají být vypracované v týmu. Díky této podmínce si studenti osahají práci v týmech a vyzkouší si pracovat tak, jak to od nich bude v praxi vyžadováno. V běžném životě, doma, či v práci je pohled na řešení problémů trochu jiný, než ve školních lavicích. V hodinách předmětu Management počítačových sítí budou studenti rozděleni do týmu a postaveni před problém. Jako tým také budou hodnoceni a podle toho jak problém vyřeší, budou odměněni daným počtem bodů. Proto, aby tým vyřešil zadané úlohy, budou muset studenti pátrat po různých postupech a řešeních. Vyučující se zde stává spíše konzultantem a rádcem.

# 1 Bezdrátové sítě

Hovoříme-li o bezdrátových sítích, mohli bychom se klidně bavit o televizním či rádiovém vysílání, stejně jako o mobilních telefonních sítích a standardu GSM, CDMA, UMTS, nebo bychom mohli hovořit o profesionálních datových sítích FWA a rádiových sítích Tetra. Všechny tyto sítě mají něco společného: k jejich provozování musí mít provozovatel nebo vlastník zakoupenou licenci vydávanou příslušným regulačním orgánem.

Licencování jednotlivých pásem má svoji logiku. Rádiových frekvencí určených pro jednotlivé služby není nekonečný počet, proto jsou označovány jako takzvané omezené zdroje, jsou přidělovány a jejich využití je zpoplatněno. Držitelé těchto licencí si svá pásma hlídají a kontrolují, jestli někdo cizí nevyužívá jim přidělené prostory v těchto pásmech.

Jelikož rádiové frekvence používá i mnoho dalších zařízení, která jsou běžně v našich domácnostech (např. mikrovlnné trouby nebo bezdrátové telefony) je hloupost, aby si každý, kdo si zakoupí přístroj využívající těchto frekvencí, musel zakoupit i pásmo, ve kterém přístroj pracuje.

Proto vzniklo pásmo s názvem ISM(Industrial Scientific and Medical) neboli pásmo vyhrazené pro vědecké, průmyslové a lékařské účely. Pásmo 2,4 GHz vymezil pro tyto účely jak americký regulátor FCC, tak evropský ETSI. Toto pásmo dříve využívaly převážně již zmiňované mikrovlnné trouby a bezdrátové telefony, ale díky rostoucímu zájmu o výpočetní techniku rychle začali toto pásmo využívat i výrobci bezdrátových sítí.

Dalším pásmem je pásmo 3,5GHz. Toto pásmo má veliké možnosti, bohužel je celé licencované. Později se začalo přecházet i na pásmo o větší frekvenci, a to o frekvenci 5 GHz.

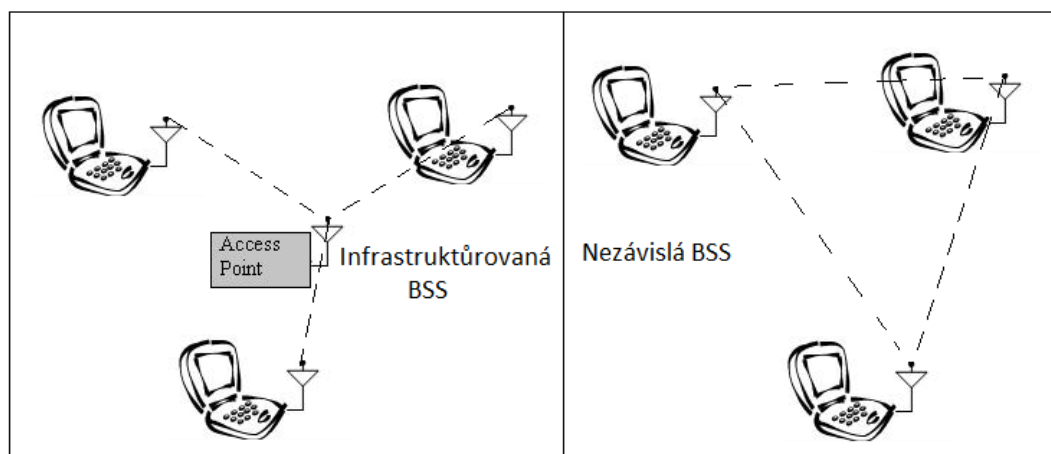
Zpočátku každý z výrobců vyráběl své vlastní technologie, ale na rozšíření technologie měl asi největší podíl izraelský výrobce BreezeNete. [ZANDL, P. 2003]

## 1.1 *Standardy WIFI sítí*

U bezdrátových sítí brzy výrobci poznali výhodu společného standardu a v roce 1997 publikoval mezinárodní standardizační institut IEEE specifikaci standardu bezdrátové sítě pracující v pásmu ISM pod číslem 802.11. Tato bezdrátová síť nabízela rychlost až 2 Mbit/s.

IEEE 802.11 je tedy WiFi standard s dalšími doplňky pro lokální bezdrátové sítě (Wireless LAN, WLAN). Výraz 802.11x je používán pro množinu doplňků k tomuto standardu. Výraz IEEE 802.11 je také spojován s původním 802.11 standardem (tedy bez dalších doplňků).

Základním stavebním kamenem 802.11 sítě je Basic Service Set (BSS). Jedná se o skupinu stanic, které spolu komunikují. Komunikace probíhá v rámci poněkud mlhavé vzdálenosti, tzv. základní oblasti služeb, která je vymezena šířící vlastností bezdrátového média. Když je stanice v základní oblasti služeb, může komunikovat s ostatními členy BSS. BSS přicházejí ve dvou typech zapojení, z nichž oba jsou znázorněny na dalším obrázku.



**Obr. 1 Basic Service Set**

Standard 802.11 se skládá ze šesti druhů modulací pro šíření radiového signálu, všechny jsou založeny na stejném protokolu. Nejrozšířenější modulace jsou takzvané dodatky k původnímu standardu a jsou označovány písmeny: „a“, „b“, a „g“. IEEE 802.11n dokáže zajistit velký dosah bez ztráty rychlosti a vylepšit odolnost vůči rušení. 802.11n přináší nové možnosti nastavitelnosti parametrů fyzické vrstvy a MAC podvrstvy pro vylepšení a zvýšení datové propustnosti. Mezi tyto nové možnosti patří změna MAC protokolů, použití většího množství antén, nebo změny kódovacích schémat. Hlavním

cílem této skupiny je dosáhnout přenosové rychlosti minimálně 100 Mbit/s nad MAC vrstvou.

K původnímu zabezpečení byl v roce 2002 přidán dodatek s novými bezpečnostními prvky. Název dodatku je zakončen písmenem „i“. Další dodatky pouze opravují nebo rozšiřují předchozí modulace.

Standard 802.11a používá 5 GHz pásmo, tudíž není tak ovlivňován jinými zařízeními jako jiné standardy. Standardy 802.11b a 802.11g používají frekvenční pásmo 2,4 GHz. Proto se mohou prolínat a navzájem rušit se zařízeními, která používají stejné pásmo. Třeba jako jsou mikrovlnné trouby, Bluetooth nebo bezdrátové telefony.

## **Přehled jednotlivých standardů WIFI sítí**

### **IEEE 802.11a**

Tento standard využívá ke své práci pásmo 5GHz. Používá modulaci OFDM [Metoda modulace OFDM je založena na využití určitého počtu (93-468) nosných kmitočtů, které jsou dále měněny různě mohutnými modulacemi.]. Naproti standardům pracujícím v pásmu 2,4 GHz je tento standard stabilnější a pokročilejší. Má povolený vyšší vyzařovací výkon, a proto se dá použít i na větší vzdálenosti.

### **IEEE 802.11b**

Tento standard byl přijat roku 1999 a oproti výchozímu standardu navyšuje přenosovou rychlost až na 11 Mbit/s v přenosovém pásmu 2,4 GHz. Přitom se dosah tohoto standardu ve volném prostředí může pohybovat až okolo 12 kilometrů. Vysílá ve frekvenčním pásmu 2400-2485 MHz.

**Tab. 1 Kanály dle standardu IEEE 802.11b**

<b>Kanál</b>	<b>Kmitočet (GHz)</b>
1	2,412
2	2,417
3	2,422
4	2,427
5	2,432
6	2,437
7	2,442
8	2,447
9	2,452
10	2,457
11	2,462
12	2,467
13	2,472
14	2,484

Kanál 14 se v České republice nevyužívá a využití třináctého kanálu se pomalu také vytrácí. Zajímavé je, že když je například použit kanál 9, ruší frekvenci kanálů 8 a 10. Proto musí technik pro zavedení další sítě zvolit jiný kanál, který nebude rušen.

Tento standard je používán v zemích, kde nejsou schváleny systémy používající jiné standardy s dodatky IEEE 802.11. Často se označuje také jako globální harmonizační standard.

### **IEEE 802.11g**

Tento standard je dá se říct rozšířením standardu IEEE 802.11b, vysílá na stejných frekvencích, ale maximální skutečná rychlost se pohybuje okolo 54 Mbit/s. To znamená, že rychlost přenosů odpovídá cca 25Mbit/s. Je zpětně slučitelný se standardem IEEE 802.11b.

### **IEEE 802.11h**

Tento standard doplňuje IEEE 802.11a, který byl zkonstruován s ohledem na evropské požadavky s možností využívat sítě i mimo budovy. Postará se například o problémy rušení jinými zařízeními, která také operují na frekvenci 5 GHz, jako jsou třeba satelitní antény nebo radary. V jádru věci má bezdrátové zařízení v případě, že detekuje rušení, omezit vysílací výkon nebo opustit kanál, u kterého toto rušení rozpoznalo.

### **IEEE 802.11i**

Tento standard je určen pro zabezpečenou komunikaci v bezdrátové síti LAN, IEEE 802.11i vylepšuje WEP (Wireline Equivalent Privacy).

### **IEEE 802.11n**

Tento standard byl zaveden v roce 2009, cílem tohoto standardu je upravit fyzickou vrstvu tak, aby bylo docíleno reálných rychlostí přes 100 Mbit/s. Využívá jak pásmo 2,4 GHz, tak i 5GHz, přičemž maximální fyzická rychlost může dosahovat i 600Mbit/s. Zvýšení rychlosti se dosahuje díky technologii MIMO (Multiple Input Multiple Output), tudíž díky využití více vysílačích i přijímacích antén.

[Zandl, P. 2003]

## **1.2 Antény, přijímače**

Antény jsou vlastně přijímače i vysílače rádiových signálů. Elektromagnetické vlnění různých frekvencí se šíří podobně jako světlo, tudíž každá překážka může buď znemožnit příjem, nebo omezit dosah tohoto vlnění. Je to podobné jako u paprsku světla, překážkou může být jak budova, tak déšť nebo mlha. Dosah signálu v uzavřených prostorách se zpravidla pohybuje mezi třiceti až padesáti metry. Přitom v nestíněných prostorách nebo volných rozsáhlých plochách se dostupnost signálu díky použití směrových antén pohybuje v rozmezí několika kilometrů. Bohužel jako daň za tuto výhodu se s narůstající vzdáleností snižuje reálná přenosová rychlost.

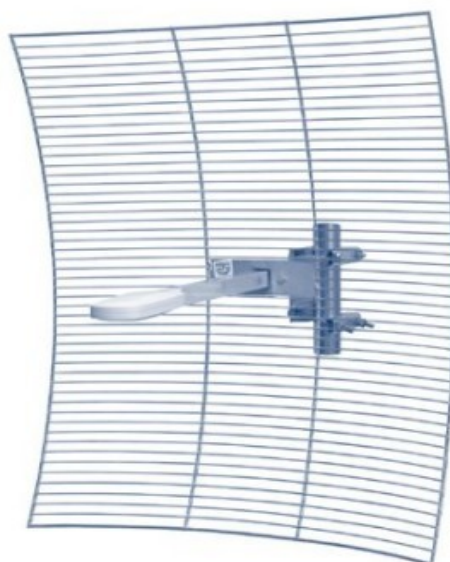
Také WiFi karta je vlastně transceiver (transmitter = vysílač, receiver = přijímač), jehož vlastnosti, jako jsou citlivost, výstupní výkon vysílače, intermodulační odolnost, spektrální čistota signálu a kmitočtová stabilita, musí odpovídat standardům, uvedeným v jistých mezinárodních standardech, ze kterých vycházejí i předpisy platné u nás.

### **1.2.1 Typy antén pro bezdrátové sítě sítí**

#### **Směrové antény**

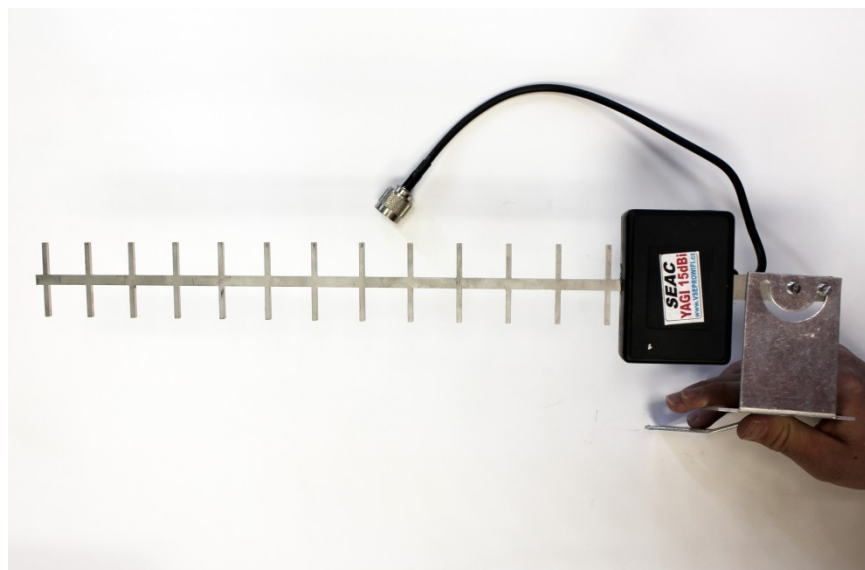
Směrové antény se používají tam, kde je potřeba dostat signál na jedno určité místo. Zpravidla je toto místo (bod) daleko, tudíž se veškerá síla antény zaměřuje na poslání nebo přijetí signálu z tohoto bodu. Jde o směrové parabolické antény.

- a) Antény typu Sito – takzvané Grid antény jsou díky svému provedení méně náchylné na povětrnostní podmínky, ale zápor se jeví v tom, že tyto antény mají vyšší šumivost.



**Obr. 2 Anténa typu Sito[ASPA, a.s.]**

- b) Antény typu Yagi – obvykle bývají obaleny ve vodotěsném pouzdru, vývojově patří mezi nejstarší typy antén, jako zápor se jeví z hlediska rušení takzvané vedlejší vyzařovací laloky.



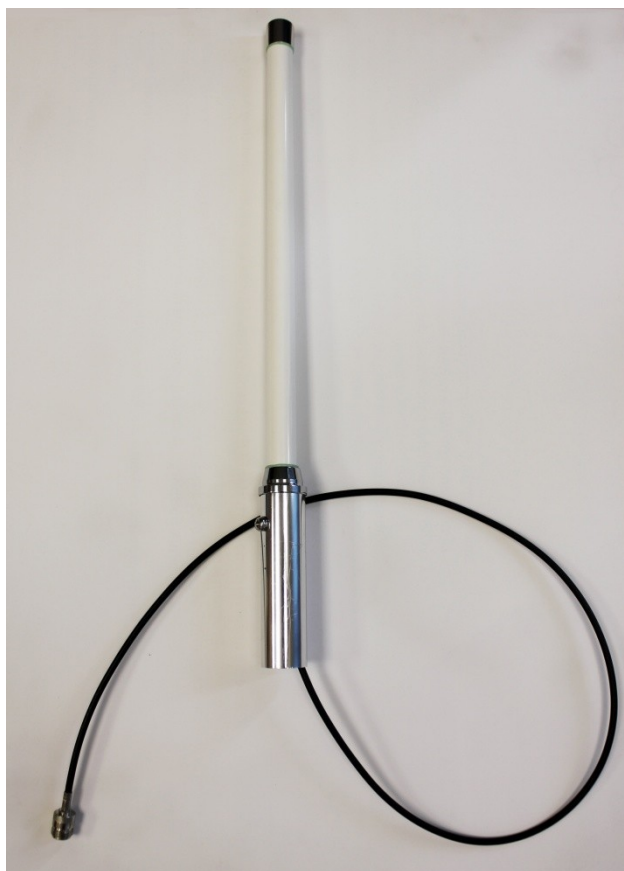
**Obr. 3 Yagi anténa**



- c) Antény typu Parabola – je to směrová anténa s takřka nejlepšími vlastnostmi. Nevýhodou je však cena a díky svému provedení náchylnost na povětrnostní podmínky.

### **Všesměrové antény**

Vykrývají úhel  $360^\circ$ , tudíž se používají tam, kde je potřeba souvislého signálu. Jsou ideální pro použití jako centrální Access Point v prostorách bez rušení. Do této skupiny patří jak klasické malé anténky dodávané s aktivními prvky, tak antény se ziskem klidně 10dB.



**Obr. 4 Všesměrová anténa**

### **Sektorové antény**

Tyto antény vyzařují do konkrétního úhlu, používají se tam, kde je potřeba vykrýt omezenou oblast. Pokrývají jak 60 stupňů, tak třeba 90 nebo 180. Záleží na konkrétním požadavku. Dalo by se říct, že antény směrové spadají pod tyto sektorové antény.



Obr. 5 Sektorová anténa

### 1.2.2 Technické parametry antén

- a) **Směrovost antény** – je to schopnost antény vyzařovat nebo přijímat elektromagnetické vlny v konkrétním směru. Posuzuje se podle takzvaných vyzařovacích charakteristik. Tyto charakteristiky se dělí na vertikální a horizontální. Vertikální = řez svislou rovinou, horizontální = řez vodorovnou rovinou.
- b) **Vyzařovací úhel antény** – je to úhel, který je dán směrovým diagramem. Počítá se jako rozdíl úhlů bodů, u kterých je pokles signálu o 3dB.
- c) **Zisk antény** – jednotkou je decibel. Říká nám, kolikrát větší výkon se musí doručit do půlvlnného dipólu, aby na místě příjmu signálu byla stejná energie jako u směrových antén. Anténa přijímající signál stejně jako dipól má zisk 0dB.
- d) **Impedance antény  $Z$**  – se udává v ohmech [ $\Omega$ ]. U bezdrátových sítí se používají antény s impedancí okolo 50 Ohmů. Je to reálná impedance bez imaginární složky.

Musí být poměrně stejná jako impedance přívodního kabelu, aby nedocházelo ke zbytečným odrazům a k nárůstu odrazového výkonu.

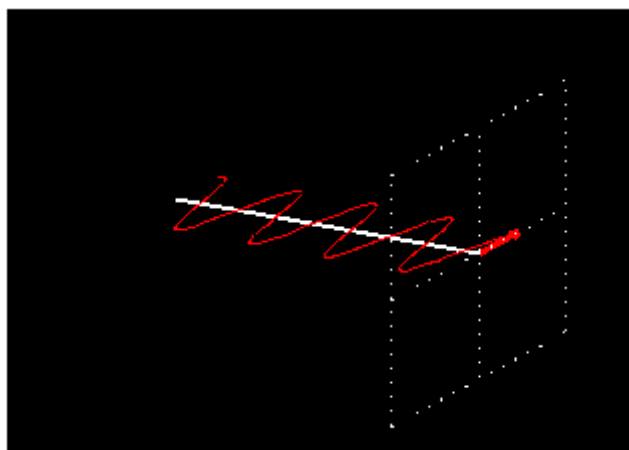
[Bartáček, J. 2009]

### 1.2.3 Polarizace antén

Pokud se bavíme o bezdrátovém přenosu, používáme dva typy polarizace elektromagnetického vlnění. Polarizace má své uplatnění například ve městech a jiných lokalitách s vysokou frekvencí bezdrátových sítí. Základní kamenem bezdrátových sítí je důležitý fakt, že pokud nechceme přicházet o signál díky útlumu, je potřeba aby anténa, kterou se signál přijímá, měla stejnou polarizaci, jako anténa, která signál vysílá.

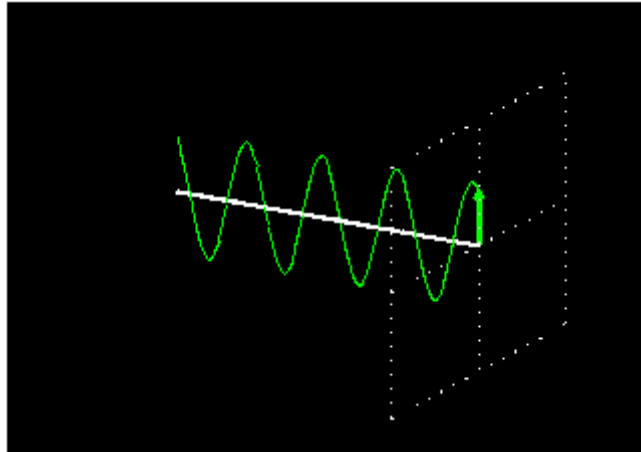
a) **Lineární polarizace** – v praxi se využívá dvou provedení:

- horizontální



Obr. 6 Horizontálně polarizovaná vlna [Mgr. Roman Pilný]

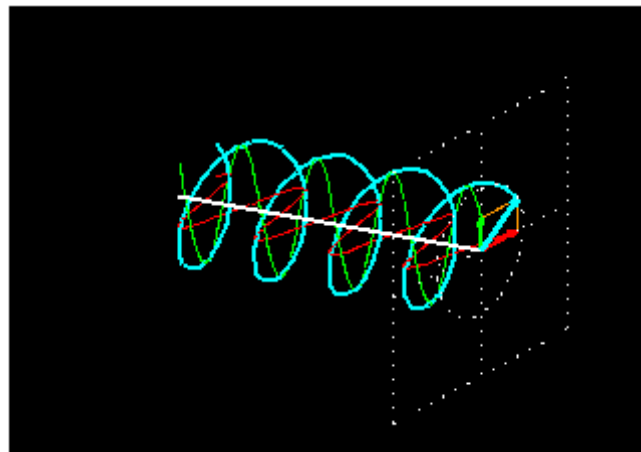
- vertikální



Obr. 7 Vertikálně polarizovaná vlna [Mgr. Roman Pilný]

b) **Kruhová polarizace** – opět se využívá dvou provedení:

- pravotočivá
- levotočivá



Obr. 8 Levotočivé polarizované vlnění [Mgr. Roman Pilný]

Pokud ovšem není prioritou velký dosah nebo optimalizace přenosové trasy, je možno použít správnou kombinaci antén. Například pokud bude signál vysílán z antény s lineární polarizací a přijímač bude šroubovicová anténa s kruhovou polarizací, bude zisk této antény o 3dB menší. Ovšem pokud bude vysílací anténa nastavená například na horizontální polarizaci a přijímač na vertikální, může se stát, že útlum zisku antény může být 16 až 24 dB. To samozřejmě znamená, že přenos dat bude omezen, nebo dokonce ochromen. U mnoha antén je možno polarizaci jednoduše změnit pootočením zářiče

o 90 stupňů. Někteří výrobci to ale nedoporučují z důvodu udržování vlhkosti na anténě a posléze změně charakteristiky antény.

U WiFi technologií se normálně používá horizontální nebo vertikální polarizace. Kruhová se využívá jen zřídka. Pokud je použita směrová anténa pro spojení dvou bodů, je lepší nastavit horizontální polarizaci. Vertikální se používá pro připojení k hlavnímu, centrálnímu bodu. Takový bod většinou používá sektorovou, nebo všesměrovou anténu s vertikální polarizací. Pokud ovšem získáváme signál, který je velice nekvalitní z důvodu velké zástavby ve městech, nebo mnoha odrazů o vodní plochy (nelze rozpoznat, jestli se jedná o vertikální nebo horizontální polarizaci), je lepší použít anténu s kruhovou polarizací. Ztráta by byla menší, než u antény s lineární polarizací.

### ***1.3 Konektory a kabely***

Antény jsou s další jednotkou samozřejmě propojeny pomocí kabeláže. Hlavním důvodem pro použití různého typu kabelu je jeho útlum.

#### **1.3.1 Kabeláž**

Větší procento antén je navrženo tak, aby byly napájené koaxiálním kabelem s impedancí 50 Ohmů. Koaxiální kabel přenáší elektrické signály pomocí dvou vodičů, středového vodiče a takzvaného „opletení“. Toto opletení slouží k tomu, aby odstiňovalo středový vodič od vlivů, které na něj mohou působit z okolí. Co se týče přenášeného signálu, ten je určen napětím mezi vodiči. Složení kabelu od středu je reprezentováno středovým vodičem, který je nejčastěji z měděného drátu, poté izolací tvořenou z pěny teflonu, dielektrika, nebo dokonce tvořené pouhým vzduchem. Následuje vodivé opletení a nakonec je celek zabalen do ochranného pláště. Je dáno, že tlustější kabel má nižší útlum.



Obr. 9 Koaxiální kabel

### 1.3.2 Náhrada koaxiálního kabelu

V dnešní době přichází trend používat místo koaxiálního kabelu různé outdoorové klienty, které lze prostě připevnit přímo k anténě. Tím odpadá potřeba použití ztrátového koaxiálního kabelu. Na zařízení není žádný napájecí jack, je napájeno přímo po UTP kabelu.



Obr. 10 UBNT Bullet2 HP, miniaturní outdoor klient 2,4GHz[ASPA, a.s.]

### 1.3.3 Konektory

Kabely jsou samozřejmě zakončeny konektory. Nejčastěji se používají dva typy těchto konektorů, konektor RSMA a konektor typu N. Revizní SMA bývá u WiFi karet, je zlacený a ve většině případů vhodný pro použití u tenčích koaxiálních kabelů. Je vhodný pro venkovní použití. Konektor typu N je vhodný jak pro menší, tak pro větší průměry koaxiálních kabelů. Může být použit i ve venkovních prostorech, je jen potřeba jej ošetřit proti vlhkosti.

[Bartáček, J. 2009]

## 1.4 *Další hardware pro bezdrátové sítě*

V této podkapitole jsou popsány jednotlivé typy bezdrátových zařízení. V dnešní době je na trhu spousta značek a spousta typů těchto zařízení.

### 1.4.1 Access Point (Bezdrátový přístupový bod)

Pro přechod mezi kabelovou a bezdrátovou sítí potřebujeme zařízení, které se jmenuje přístupový bod, anglická zkratka je AP. AP posílá všechna data jak po „pevné síti“, tak i bezdrátově. Zařízení má konektor (RJ-45) pro připojení do sítě. U AP nejde s jistotou určit maximální počet klientů. Vždy záleží na určitém přístroji. Důležitým údajem je množství přenesených dat. Tato data se dají samozřejmě zašifrovat tak, aby je mohlo přečíst jen zařízení, které má správný klíč.



Obr. 11 OvisLink WLA-5200AP 5GHz 802.11 a/b/g 6 mode AP [ASPA, a.s.]

### 1.4.2 Router

Router se stará o přístup k internetu. Stará se o předávání dat z internetu jednotlivým počítačům a naopak. Dá se říci, že je to takový most mezi dvěma sítěmi. Mezi Internetem a naší sítí.



**Obr. 12 AirLive GW-300R 802.11b/g/n Gigabit Router/ 4x LAN 1000 Mbps/ 1x WAN 1000Mbps, 2T2R, IPTV[ASPA, a.s.]**

### 1.4.3 Wireless Bridge

Klasické AP má velice omezené funkce, sice dokáže připojit k síti počítače, ale nedokáže propojit třeba dvě bezdrátové sítě. Z tohoto důvodu využíváme toto zařízení. Je to jakýsi most, díky kterému se dají spojit dvě různé bezdrátové sítě. Také se může využívat jako pomůcka pro zvětšení dosahu bezdrátové sítě. Počítač se může připojit k síti se stejnými parametry, ale k jinému AP, tento bridge dokáže tyto přístupové body propojit a tak vytvořit síť s větším dosahem. Tato metoda se nazývá roaming. [Köhre, T. 2004]





**Obr. 13 AirLive WLA-9000AP 802.11a, AP/Bridge [ASPA, a.s.]**

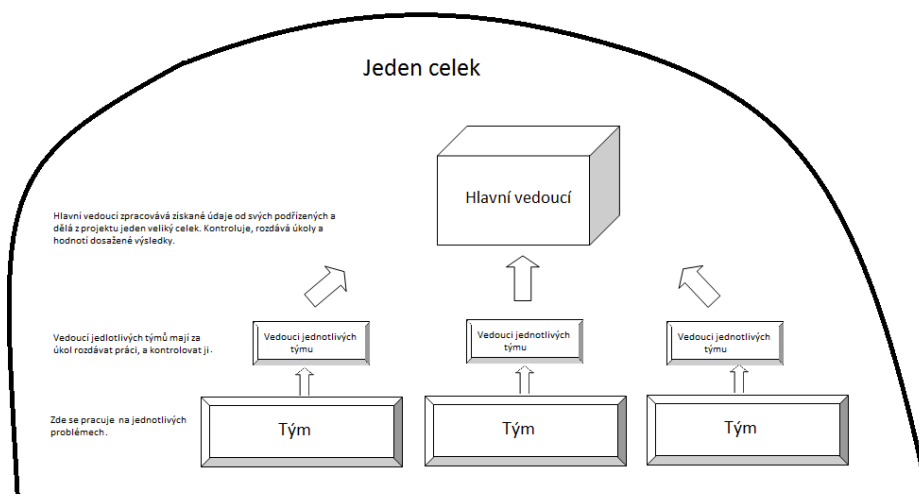
## 2 Problematika týmové práce

Základním bodem úspěchu je vytvoření dobře pracujícího týmu. V každém týmu by měl být jeden vedoucí, který rozdělí práci na projektu do určitých částí, které následně přidělí svým spolupracovníkům. Důležitou vlastností týmu je schopnost komunikovat, bez tohoto prvku by týmová práce nemohla fungovat. V dnešní době je potřeba, aby lidé s vysokoškolským vzděláním dokázali pracovat v týmech, protože v průmyslu je to již samozřejmostí.

Základní schopnosti člověka potřebné pro správnou funkci týmu jsou následující:

- a) schopnost spolupracovat,
- b) schopnost racionálně přemýšlet,
- c) schopnost ustanovit si priority,
- d) schopnost komunikovat,
- e) schopnost vybrat to správné řešení,
- f) umění naslouchat.

Problém může nastat tehdy, když je tým složen z různorodých lidí, kteří se nedokážou domluvit. Je-li tým rozdělený na více menších týmů, ve kterých lidé spolupracují na řešení určitého problému, je potřeba aby postupné výsledky a zjištění předkládali svému vedoucímu. Ten se musí postarat o to, aby se tyto informace dostaly hlavnímu vedoucímu, který má za úkol posbírat veškeré dosažené výsledky ze všech týmů a skloubit je dohromady tak, aby vznikl celek. To směřuje k tomu, aby byl problém nebo úkol vyřešen. Proto, aby byla práce efektivní, je důležité dodržovat zaběhnuté postupy a zbytečně se nerozptylovat jinou činností. Pokud ovšem tým vymýšlí, nebo zpracovává něco nového, je potřeba vše správně promyslet, rozdělit práci a fungovat jako jeden velký celek. Pokud se v týmu objeví jeden nebo dva problémoví členové, kteří nedokážou spolupracovat, je potřeba tento problém eliminovat. Eliminace problému je základ úspěchu. Takto problémový člen se bude muset buď aklimatizovat a dostat do toho správného pracovního koloběhu, nebo jej bude muset opustit. V našem případě nedokončit tento předmět.



Obr. 14 Hierarchie složeného pracovního týmu

## 2.1 Pravidla dobrého týmového rozhodování

Máme určitá daná pravidla, která bychom měli dodržovat, pokud chceme docílit správného výsledku. Tato pravidla se dělí na čtyři fáze, kterých se musí správný tým vždy držet.

1. **Dobrá otázka** (je dobré položit si správnou otázku, otázku která nám udá směr, co vlastně chceme udělat a jak to chceme udělat).
2. **Pomoci týmu vytvořit alternativy** (konkurence v myšlenkách je dobrá, v lidech ovšem pro tým destruktivní).
3. **Posoudit nebezpečí a podívat se na příležitosti** (pokud máme vymyšlené různé druhy řešení, je dobré je porovnat a vybrat to nejlepší).
4. **Rekapitulace a rozhodnutí** (jaké šance má každá verze na úspěch, zvážit rizika a přínos).

## 2.2 Základní typy rolí

Práci týmu by dokázal zvládnout i jeden člověk, ovšem musel by být dokonalý. To znamená, že dokonalý člověk by měl být:

- otevřený,
- metodický,
- motivující,

- tvořivý,
- usilovný,
- objektivní,
- diplomatický,
- pečlivý,
- inteligentní.

Člověk, který by měl všechny tyto vlastnosti, ale nejspíš neexistuje, proto je potřeba, aby byl tým složen alespoň ze dvou lidí.

Každý člen týmu působí ve dvou rolích:

1. **Funkční role** – záleží na zkušenostech a schopnostech člověka.
2. **Týmová role** – tendence chovat se, schopnosti přispívat celku a vytvářet vztahy s ostatními.

## 2.3 *Typy týmových rolí*

V první řadě je důležité sestavit takový tým, ve kterém budou zastoupeny všechny týmové role.

Dalším krokem je zvážit konstrukci týmu tak, aby vztahy mezi různými týmovými rolemi dávaly vyniknout silným stránkám a slabé potlačovaly.

V neposlední řadě je důležité se zaměřit na to, aby členové týmu postupně pochopil i silné a slabé stránky ostatních.

### **Rozdělení lidí v týmu podle jejich rolí, klady a zápory:**

#### **Vyhledavač zdrojů**

- + Přímá povaha, rychle si osvojuje nové myšlenky.
- Není-li stimulován ostatními, může se brzy začít nudit.

#### **Realizátor**

- + Je ukázněný a postupuje metodicky.
- Tendence k nepružnosti.

**Koordinátor**

- + Vychází dobře s lidmi a dostává z nich to nejlepší.  
Motivuje ostatní.
- Tendence nechat se zmanipulovat.

**Myslitel**

- + Je chytrý a tvořivý.
- Nekonformita.

**Formovač**

- + Je usilovný, pozitivní a náročný.
- Má tendenci jednat bez obalu až hrubě.

**Koordinátor – vyhodnocovač**

- + Je opatrný a má ke všemu objektivní přístup.
- Bohužel je pomalý a neinspirativní.

**Týmový pracovník**

- + Je nápomocný ostatním a diplomat.
- Může být nerozhodný v krizových situacích.

**Kompletovač**

- + Je pečlivý, důsledný a pozorný k detailům.
- Má přehnané tendence k obavám.

**Specialista**

- + Tento člověk má hluboké vědomosti a je zaujatý pro věc.
- Jeho přínos je omezen jeho odborností.

### **3 Předmět Management počítačových sítí**

Tento předmět je určen studentům posledního navazujícího ročníku, a proto je v něm kladen důraz na doplnění znalostí (a případných mezer v nich) v oblastech vyžadovaných v praxi, na které nebylo během studia ostatních předmětů dostatek času ani prostoru. Jeho hlavním cílem je seznámit budoucí inženýry s nejnovějšími technologiemi používanými v praxi z oblasti přeměny, prezentace a zpracování dat.

Definice je uvedena [VSB-TUO]

Základním kamenem tohoto předmětu je myšlenka zavedení revolučního učebního postupu, který je založen na tom, že se studenti od praktických pokusů postupně dostanou až k základům teorie. Jednoduše řečeno, teoretickou část problému si dokážou sami odvodit díky znalosti a praktického odzkoušení problému.

„Studenti tak budou mít ucelený přehled v informačních technologiích postavených na jazyku XML, databázových technologiích a také se seznámí s jedinečnou problematikou stavění bezdrátových WiFi sítí. Studenti tak získají schopnosti tyto technologie efektivně zhodnotit, kvalifikovaně rozhodnout kdy a jakou technologii použít, navrhovat a tvořit postupy vedoucí ke zdárnému získávání a transformaci dat ze sdílených datových zdrojů. V neposlední řadě získají schopnost navrhovat a vybudovávat bezdrátové WiFi sítě s ohledem na problematiku šíření rádiového signálu.“

#### **Anotace k předmětu**

„Cílem předmětu je doplnění znalostí v oblasti vývoje aplikací úzce svázaných se síťovými technologiemi a budování WiFi sítí. Předmět pokrývá 5 tematických okruhů: technologie XML, jazyk SQL DML, Microsoft SQL Server, vývoj databázových klientů pomocí ADO.NET a problematika budování WiFi sítí.“

[VSB-TUO]

## O předmětu Management počítačových sítí

V této práci se budu zaměřovat na poslední týdny výuky tohoto předmětu, tudíž se zaměřím na problematiku WiFi a zpracuji různé postupy a návrhy jak se naučit správně využívat tuto technologii.

**Tab. 2 Obsah předmětu**

1	Jazyk XML
2	Technologie XML
3	Dotazování nad dokumenty XML (XQuery, Linq To XML)
4	Microsoft SQL Server z pohledu správy a tvorby databází, úvod k jazyku Transact SQL
5	SQL DML: získávání dat
6	SQL DML: souhrny a seskupování dat
7	SQL DML: dotazy nad vícero tabulkami
8	SQL DML: modifikace dat a fulltextové vyhledávání
9	Programové prostředky: uložené procedury, spouště, uživatelské funkce
10	Tvorba tlustých klientů v ADO.NET II (VB.NET nebo V#)
11	Technologie WiFi: komponenty, typy sítí, dostupné frekvence
12	Hardware pro WiFi sítě: přístupové body, antény, kabely, konektory apod.
13	Plánování sítě: problematika šíření WiFi signálu, zabezpečení

## 4 Návrh týmových úloh pro předmět Management počítačových sítí

Pro inovaci předmětu Management počítačových sítí, který se v posledních hodinách výuky zaměřuje na technologii WiFi a problematiku týmové práce, byly navrženy tři nové týmové úlohy. Tyto úlohy sledují dva cíle:

- 1) seznámit studenty s praktickým vybudováním WiFi sítě, jejich zabezpečením a dalšími možnostmi jeho využití,
- 2) prakticky seznámit studenty s prací v týmech.

Pro naplnění cíle 2 bude každá úloha řešena studenty sestaveným týmem.

### **Základními úkoly týmů budou:**

- a) po zadání úlohy je potřeba rozvrhnout práci členům týmu tak, aby splnění bylo efektivní,
- b) tým provede zadanou úlohu a vytvoří protokol o této úloze,
- c) tým vypracuje protokol o zhotovené úloze, poté vypracuje prezentaci, kterou bude prezentovat ostatním studentům ve třídě.

### **4.1 Úloha: Správné umístění antény přístroje v prostorách bytu**

Cílem této úlohy je naučit studenty, jak správně umístit anténu v prostorách bytu a jak se správně naučit pracovat v malém týmu tak, aby byla práce efektivní. Důležitým faktem pro stabilitu spojení a datovou propustnost je schopnost antény poradit si s horšími podmínkami, např. s různými překážkami. Ty se nejvíce podepíší na celkové přenosové kapacitě.

#### **Skladba týmu**

Úloha je připravena pro tříčlenný tým studentů. Tento tým bude měřit sílu signálu v určených prostorách. Jeden člen týmu se zaměří na práci s routerem, další dva na práci s PDA. Po získání potřebných dat tým vytvoří protokol k zadané úloze.



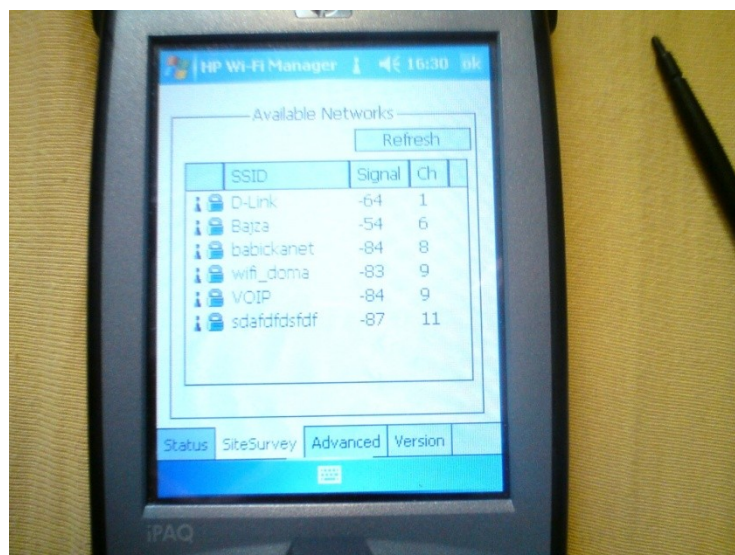
## Zadání úlohy

- 1) První student zprovozní a nastaví router.
- 2) Druhý a třetí student měří sílu signálu pomocí přenosného PC, nebo PDA a softwarového nástroje k tomu určeného. Měření provádějí v daných zónách. Měření opakují.
- 3) V protokolu sepiší zjištěné poznatky a vytvoří graf.

### Budeme provádět měření ve třech zónách:

- V zóně přímé viditelnosti na anténu přístroje, což je ve vzdálenosti cca 1,5 m od krabičky. Toto měření ukazuje použitelnost v místnosti, ve které se router nachází.
- Další zónu nazveme zónou za zdí, což je dosah za třemi zdmi se zavřenými dveřmi. Toto měření odpovídá použitelnosti v rohu bytu.
- Třetí a poslední zónu nazveme zónou velice špatných podmínek. Tato zóna je vzdálená asi tři zdi a půl poschodí od krabičky. Zde některé antény routeru dokonale zklamou (přenosová rychlost klesne až na 0 Mbit/s). Je to způsobeno tím, že signálu stojí v cestě železobetonový strop, stěny i schodiště.

V každé zóně opakujeme měření třikrát, čtyřikrát. A to proto, abychom dostali výsledky s minimální odchylkou.

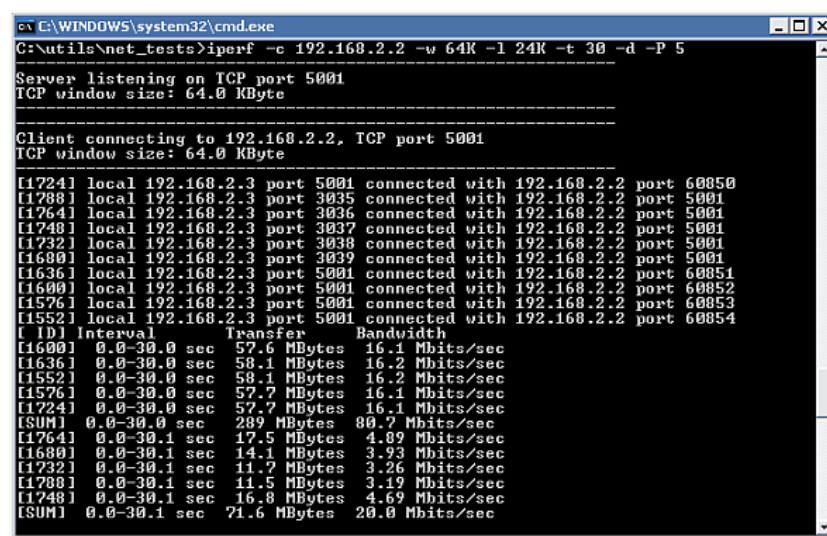


Obr. 15 Použití WiFi manageru v PDA

## Měření pomocí nástroje iperf

Pokud pro měření a testování schopností antény bezdrátového routeru použijeme přenosný počítač, můžeme použít některý z nástrojů pro síťové přenosy. Například nástroj iperf.

[Extra Publishing, s. r. o. 2007–2011]



```
C:\WINDOWS\system32\cmd.exe
C:\utils\net_tests>iperf -c 192.168.2.2 -w 64K -l 24K -t 30 -d -P 5

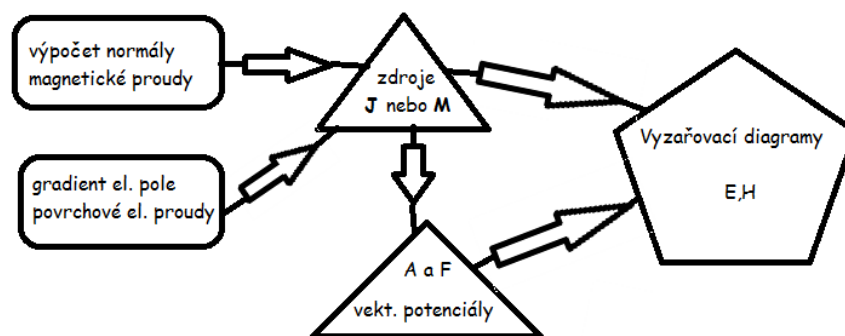
Server listening on TCP port 5001
TCP window size: 64.0 KByte

-----
Client connecting to 192.168.2.2, TCP port 5001
TCP window size: 64.0 KByte
-----
[1724] local 192.168.2.3 port 5001 connected with 192.168.2.2 port 60850
[1700] local 192.168.2.3 port 3035 connected with 192.168.2.2 port 5001
[1764] local 192.168.2.3 port 3036 connected with 192.168.2.2 port 5001
[1748] local 192.168.2.3 port 3037 connected with 192.168.2.2 port 5001
[1732] local 192.168.2.3 port 3038 connected with 192.168.2.2 port 5001
[1680] local 192.168.2.3 port 3039 connected with 192.168.2.2 port 5001
[1636] local 192.168.2.3 port 5001 connected with 192.168.2.2 port 60851
[1600] local 192.168.2.3 port 5001 connected with 192.168.2.2 port 60852
[1576] local 192.168.2.3 port 5001 connected with 192.168.2.2 port 60853
[1552] local 192.168.2.3 port 5001 connected with 192.168.2.2 port 60854
[ ID] Interval      Transfer      Bandwidth
[1600] 0.0-30.0 sec  57.6 MBytes  16.1 Mbits/sec
[1636] 0.0-30.0 sec  58.1 MBytes  16.2 Mbits/sec
[1552] 0.0-30.0 sec  58.1 MBytes  16.2 Mbits/sec
[1576] 0.0-30.0 sec  57.7 MBytes  16.1 Mbits/sec
[1724] 0.0-30.0 sec  57.7 MBytes  16.1 Mbits/sec
[SUM]  0.0-30.0 sec  289 MBytes  80.7 Mbits/sec
[1764] 0.0-30.1 sec  17.5 MBytes  4.09 Mbits/sec
[1680] 0.0-30.1 sec  14.1 MBytes  3.93 Mbits/sec
[1732] 0.0-30.1 sec  11.2 MBytes  3.26 Mbits/sec
[1700] 0.0-30.1 sec  11.5 MBytes  3.19 Mbits/sec
[1748] 0.0-30.1 sec  16.8 MBytes  4.69 Mbits/sec
[SUM]  0.0-30.1 sec  71.6 MBytes  20.0 Mbits/sec
```

Obr. 16 Použití testovacího nástroje iperf [Extra Publishing, s. r. o. 2007–2011]

## Vyzařovací diagram

Obecně se anténa vyznačuje tím, že vysílá, nebo přijímá elektromagnetickou energii. Zobrazení těchto pochodů se nazývá vyzařovací diagram pro vysílací antény a směrový diagram pro antény, které signál přijímají. Výpočet vyzařovacího diagramu je odvozen z Maxwellových rovnic. Pro každý výpočet je potřeba znát rozložení hustoty elektrických proudů  $\mathbf{J}$  na povrchu antény. Často se ovšem využívá smyšlená magnetická proudová hustota  $\mathbf{M}$ . Nejčastěji se zavádějí takzvané potenciály, které nám zjednoduší vztahy vzniklé Maxwellovými rovnicemi.



Obr. 17 Možné přístupy k výpočtu vyzařovacího diagramu

[Mudroch, M. 2011]

## 4.2 Úloha: Vytvoření firemní sítě

Cílem této úlohy je naučit studenty propojit dvě na sobě nezávislé sítě pomocí VPN tunelu. Dále si zde studenti procvičí nastavení a zabezpečení sítě vytvořené pomocí WiFi technologií.

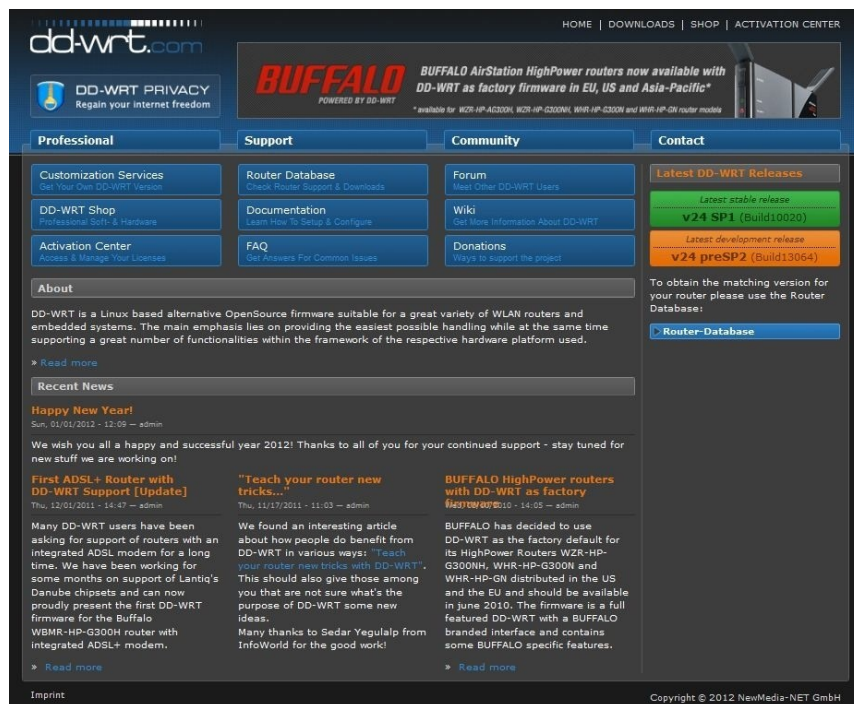
### Skladba týmu

Tato práce je vhodná pro tým o pěti studentech. Tým se rozdělí do dvou skupin, každá skupina připraví jeden z routerů, tak aby vznikly dvě různé sítě. Poté tým nastaví routery tak, aby mezi sebou mohli komunikovat, a tak vznikla možnost propojit dvě různé sítě.

### Zadání úlohy

- 1) Dva členové týmu vytvoří samostatnou WiFi síť, kterou zabezpečí známými způsoby.
- 2) Další dva členové týmu také vytvoří samostatnou WiFi síť.
- 3) Jako tým mají studenti za úkol tyto dvě sítě propojit pomocí VPN(propojit dvě různé sítě s různými IP adresami).
- 4) Poslední člen týmu sestaví prezentaci a vysvětlí ostatním studentům způsoby a problémy řešení této úlohy.

- 5) Tým vytvoří protokol k zadané úloze.



Obr. 18 Webový portál [www.dd-wrt.com](http://www.dd-wrt.com)

### 4.3 Úloha: Zabezpečení a prolomení bezdrátové sítě

Cílem této úlohy je ukázat studentům různé způsoby zabezpečení bezdrátových sítí a také studenty naučit prolomit síť s velice nízkým zabezpečením. Tým se rozdělí do dvou skupin, skupina obranářů bude mít za úkol obsluhovat přidělený router a skupina útočníků zase PC, se kterým se nabourají do vytvořené sítě.

#### Skladba týmu

Tým studentů se může skládat až z šesti členů. Dva až tři členové postupně budou nastavovat router s různým typem zabezpečení. Tři až čtyři členové budou se zase toto zabezpečení pokoušet obejít.

#### Zadání úlohy

- První tým splní tyto body zadání:
  - 1) Členové týmu mají za úkol prostudovat přiložený tutoriál, ve kterém se dozvědí, jaké máme druhy zabezpečení WiFi sítě.

- 2) Připojí k počítači přidělený hardware a vytvoří WiFi síť.
- 3) Dále zvolí a nastaví dvě metody zabezpečení. První bude jednodušší, taková, která je sice velice běžná, ale málo robustní a opravdu nedostačující. Druhá metoda zabezpečení bude taková, která bude více vhodná pro znesnadnění připojení se do bezdrátové sítě nezvaným uživatelům.
- 4) Jeden člen týmu nastaví počítač s WiFi kartou tak, aby se do této sítě bez problémů připojil.
- 5) Jako poslední bod studenti vypracují zprávu o vyhotovené práci.

*Druhý tým dostane za úkol zaútočit na tuto síť a pokusí se prolomit její ochranu.*

- Zadání bodů pro druhý tým:
  - 1) Studenti mají za úkol prostudovat přiložený tutoriál.
  - 2) K práci budou využívat notebook s operačním systémem Windows nebo Linux.
  - 3) Jako poslední bod vypracují zprávu o vyhotovené práci.

## 5 Realizace zadaných úloh

V této kapitole se podíváme na konečnou realizaci zadaných úloh.

### 5.1 Realizace zabezpečení a prolomení bezdrátové sítě

Každá vytvořená WiFi síť má různé možnosti zabezpečení.

#### Typy zabezpečení WiFi sítě

V dnešní době je na prvním místě mobilita. Internet lze užívat v mobilním telefonu, na zahradě, nebo kdekoliv v domě. Všechna tato připojení mají jednu společnou věc, a tou je přenosové médium, kterým je vzduch. Otázkou zůstává, že když se tyto vlny plachtí vzduchem, ve kterém jsme i my – je možnost si tyto vlny odchytil? Když už takové vlny vysíláme, je dobré je nějak zabezpečit proti nezvaným posluchačům.

- *Kontrola MAC-adres*

Často používaná, ale bohužel velice podceňovaná je metoda omezení přístupu pomocí MAC-adres. Při připojení je MAC adresa přenášena v nezašifrovaném tvaru, tudíž kdokoliv, kdo vlastní nějaký program pro odposlech sítě získá sledovanou MAC adresu během několika málo sekund. Poté je otázkou minuty než si nastaví na svém PC stejnou a připojí se do dané sítě pod rouškou počítače ze sítě, telefonu, tabletu nebo PDA.

- *Zabezpečení pomocí protokolu WEP*

V dnešní době jsou způsoby jak toto šifrování do hodinky bez problémů prolomit. (Například pomocí programu Aircrack). Nezáleží na tom, zda použijeme 64-bitové nebo 128-bitové heslo statické nebo s rotací. Ve finále hacker tuto síť tak i tak prolomí.

- *Zabezpečení pomocí protokolu WPA a WPA2*

Protokol WPA je pro domácnost poměrně dostatečný, i když pokud by měl být použitý k zabezpečení nějaké důležité sítě, je v tomto protokolu několik bezpečnostních mezer. WPA používá 128-bitový šifrovací klíč. Silnější a asi nejlepší je WPA2-PSK (tedy WPA zabezpečení s Pre-SharedKey).

## Dvě možnosti šifrování

### 1. Šifrování pomocí TKIP (Das Temporal Key Integrity Protocol)

Pro odstranění slabých míst byl vyvinut protokol, který se na nějakou chvíli vypořádal s problémem s inicializačními vektory a zavedl dynamickou správu šifrovacích klíčů. Tyto klíče jsou pomocí tohoto protokolu přenášeny mezi přístupovým bodem a klientem nejen na začátku komunikace, ale i během ní.

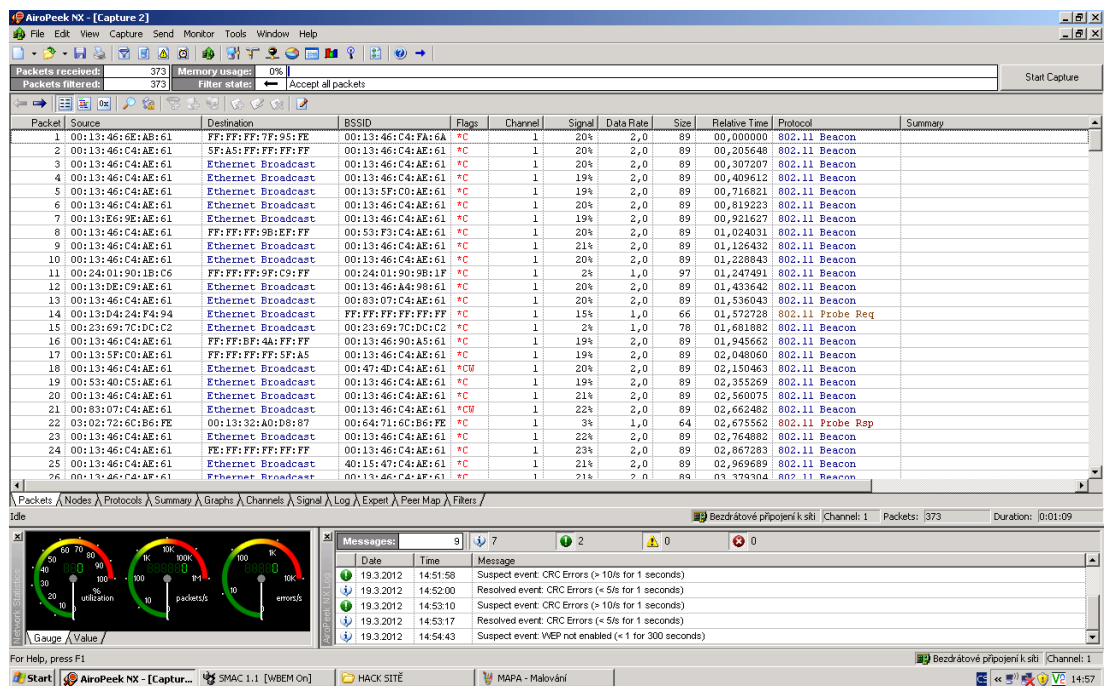
### 2. Šifrování pomocí AES (Advanced Encryption Standard)

AES má pevně danou velikost bloků (128 bitů), i velikosti klíče (128, 192 nebo 256 bitů). Pro šifrování i dešifrování používá totožný klíč na data s pevně danou délkou bloku. Toto šifrování je určitě kvalitnější, ale ne každé zařízení, zejména starší, jej podporuje.

Pro demonstraci vytvořme bezdrátovou síť s primitivním zabezpečením pomocí MAC adresy a poté zabezpečení kvalitní pomocí WPA2-PSK, šifrováním AES a 10timístným různorodým heslem.

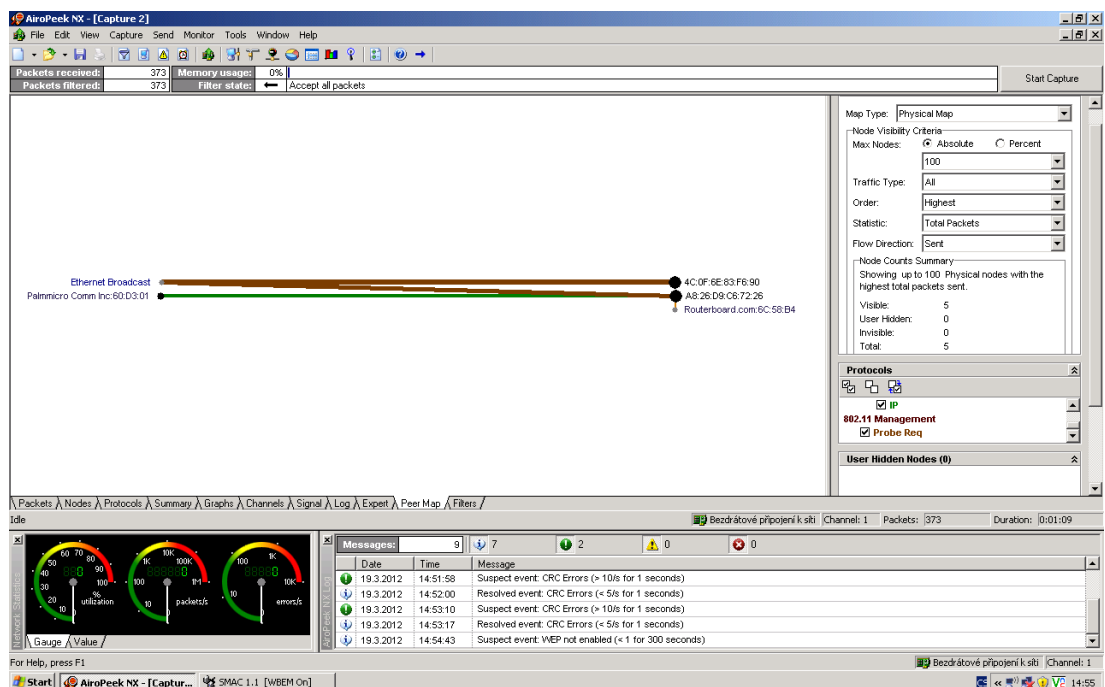
## Monitoring sítě pod Windows XP

- První věc, kterou musíme udělat je připravit si vhodně síťovou WiFi kartu, se kterou pak budeme danou síť scanovat. S běžným ovladačem Intel 10.5.1.72 lze zprovoznit bezdrátový adapter v monitoring módu. Testovaná verze ovladačů podporuje scan daného rozsahu kanálu, kde je nutno zadat alespoň dva kanály, nebo scanování všech dostupných kanálů na frekvenci 2,4– 5GHz. Po instalaci správné verze ovladače (10.5.1.72) pracuje karta na platformě Windows v monitoring módu.
- Spustíme program AiroPeek NX a zvolíme síť, kterou chceme scanovat. Poté spustíme scan. Kdykoliv je na síti nějaký pohyb AiroPeekscanuje a ukládá packety létající mezi klientem a přístupovým bodem.



Obr. 19 Ukládání packetu v AiroPeek

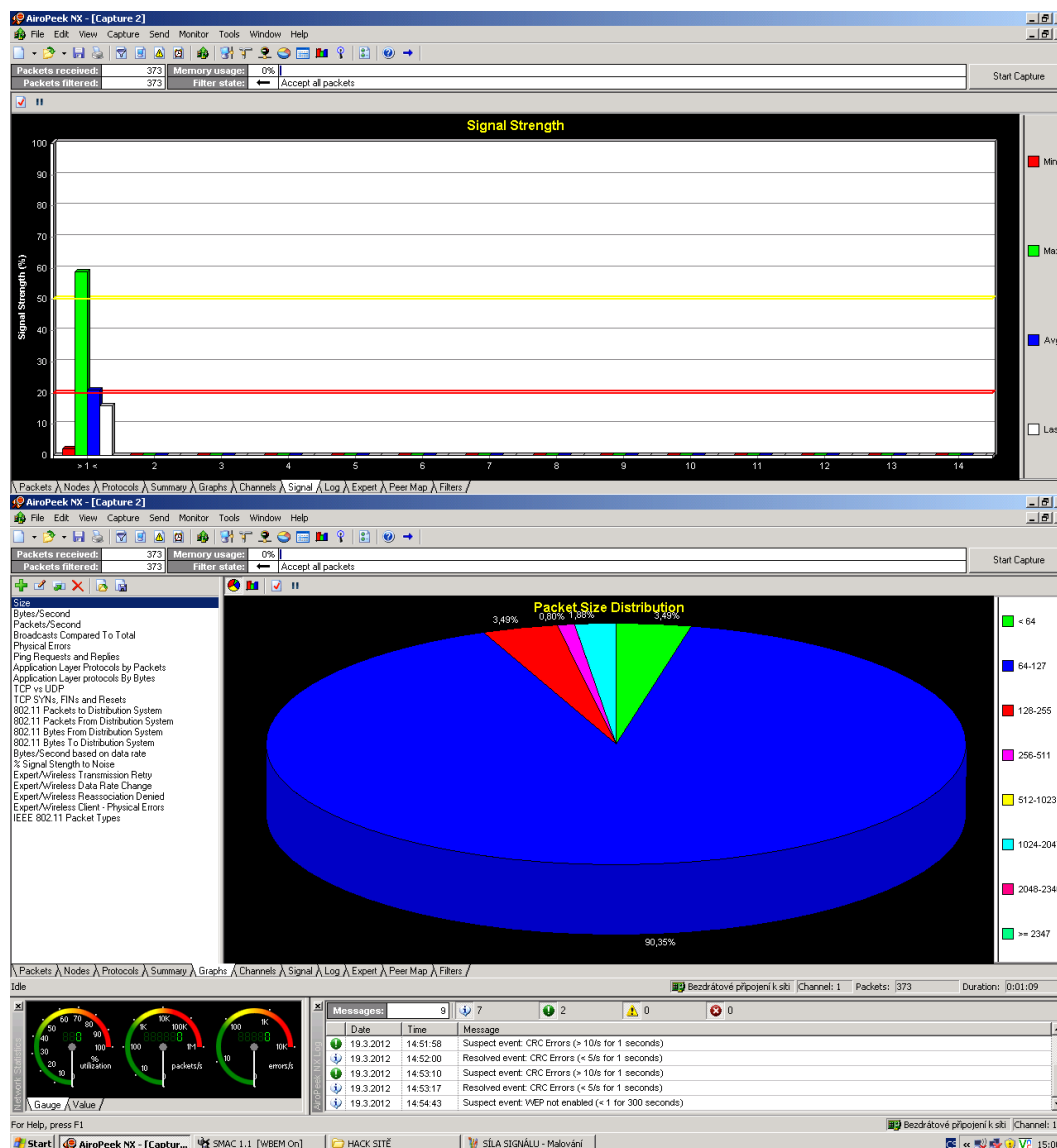
Po odchycení dostatečného množství packetů nám AiroPeek sám ukáže, kolik zařízení je v síti momentálně připojeno a dokonce nám vypíše i MAC adresy těchto klientů.



Obr. 20 Mapa zařízení připojených do sítě

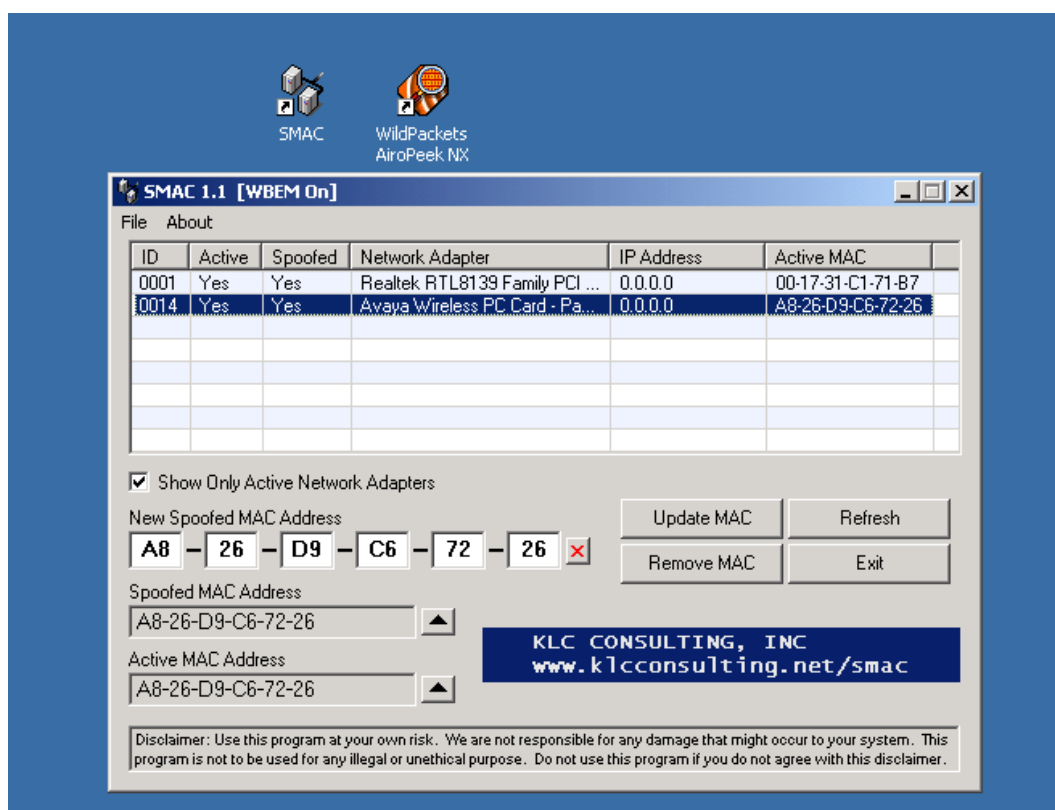


Nástroj AiroPeek má samozřejmě spoustu dalších užitečných vlastností. Můžeme zde zjistit sílu signálu nebo třeba velikosti odchycených packetů.



Obr. 21 Zobrazení síly signálu a velikosti odchycených packetu v program AiroPeek

- Teď když již máme zjištěné potřebné informace, jediné co musíme udělat, je programově změnit naší MAC adresu a nahradit jí některou z podporovaných adres v síti. K tomu slouží jednoduchý program SMAC.



Obr. 22SMAC program pro změnu MAC adresy

Po splnění těchto jednoduchých dílčích úloh můžeme libovolně surfovat v síti, která je zabezpečena pouhým tříděním klientů pomocí MAC adresy.

### Další možné typy řešení:

Pokud bychom měli prolomit síť se zabezpečením pomocí různého šifrování, například WPA nebo WEP, můžeme použít aplikaci WEPKR (WEP Key Recovery). Tato aplikace je součástí programu **CommView**. Tuto aplikaci spustíme a vybereme MAC adresu daného WiFi vysílače. Program ihned odchytává packety a následně zjistí heslo. Na stejném principu pracuje i aplikace **Aircrack-ng**, která krom WEP zabezpečení dokáže prolomit i novější zabezpečení jako je WPA-PSK.

Mezi další zajímavé programy pro detekci a zjišťování informací na bezdrátových sítích patří program Network Stumbler, nebo XirrusWiFiInspector.

## **5.2 Realizace úlohy vytvoření firemní sítě**

Provedeme zálohu a poté aktualizaci firmware routerů od neoficiálního dodavatele firmware. Například z webových stránek <http://dd-wrt.com>. Po aktualizaci provedeme nastavení routeru:

- nastavíme router přístupný jen pro určité pevné IP nastavené na PC,
- nastavíme zabezpečení bezdrátové sítě, omezení provozu bezdrátové sítě na MAC adresy a web kontroly (není potřeba, aby měli studenti a zaměstnanci přístupný veškerý obsah webu),
- dále nastavíme propojení mezi dvěma routery tak, abychom mohli zároveň pracovat ve dvou odlišných sítích.

### **Nastavení VPN tunelu**

Pro demonstraci této úlohy byly použity dva routery značky Asus s označením WL-500g Deluxe. Základní firmware byl nahrazen firmwarem od neoficiálního dodavatele ze stránek [www.dd-wrt.com](http://www.dd-wrt.com).

## Nastavení serveru

V kolonce **Basic Setup** nastavíme jméno routeru (server). Dále nastavíme IP adresy, na kterých pojede vnitřní síť

**Setup** | Wireless | Services | Security | Access Restrictions | NAT / QoS | Administration | Status

**Basic Setup** | DDNS | MAC Address Clone | Advanced Routing | VLANs | Networking | EoIP Tunnel

**WAN Setup**

**WAN Connection Type**

Connection Type: Automatic Configuration - DHCP

STP: ☐ Enable ☒ Disable

**Optional Settings**

Router Name: server

Host Name: server

Domain Name:

MTU: Auto 1500

**Network Setup**

**Router IP**

Local IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

Gateway: 0.0.0.0

Local DNS: 0.0.0.0

**Network Address Server Settings (DHCP)**

DHCP Type: DHCP Server

DHCP Server: ☒ Enable ☐ Disable

Start IP Address: 192.168.1.100

**Help** more...

**Automatic Configuration - DHCP:**  
This setting is most commonly used by Cable operators.

**Host Name:**  
Enter the host name provided by your ISP.

**Domain Name:**  
Enter the domain name provided by your ISP.

**Local IP Address:**  
This is the address of the router.

**Subnet Mask:**  
This is the subnet mask of the router.

**DHCP Server:**  
Allows the router to manage your IP addresses.

**Start IP Address:**  
The address you would like to start with.

**Maximum DHCP Users:**  
You may limit the number of addresses your router hands out. 0 means only predefined static leases will be handed out.

Obr. 23 Nastavení Basic Setup pro server

V kolonce **Advancedrouting** nastavíme veřejnou adresu routeru (od poskytovatele připojení k internetu), se kterým se chceme spárovat a dále nastavíme síť, na kterou je daný router nastavený.

dd-wrt.com ... control panel

Firmware: DD-WRT v24-sp2 (08/07/10) vpn  
Time: 08:40:44 up 7 min, load average: 0.05, 0.11, 0.07  
WAN IP: 192.168.123.6

Setup Wireless Services Security Access Restrictions NAT / QoS Administration Status

Basic Setup DDNS MAC Address Clone **Advanced Routing** VLANs Networking EoIP Tunnel

**Advanced Routing** Help more...

**Operating Mode**

Operating Mode Gateway

**Static Routing**

Select set number 1 (192.168.123.2) Delete

Route Name 192.168.123.2

Metric 0

Destination LAN NET 192.168.2.0

Subnet Mask 255.255.255.0

Gateway 192.168.2.1

Interface ANY

Show Routing Table

Save Apply Settings Cancel Changes

**Operating Mode:**  
If the router is hosting your Internet connection, select *Gateway* mode. If another router exists on your network, select *Router* mode.

**Select set number:**  
This is the unique route number, you may set up to 50 routes.

**Route Name:**  
Enter the name you would like to assign to this route.

**Destination LAN NET:**  
This is the remote host to which you would like to assign the static route.

**Subnet Mask:**  
Determines the host and the network portion.

Obr. 24 Nastavení Advanced Routing pro server

Dále budeme pokračovat s nastavením v Services – VPN – PPT Server. Zde nastavíme DNS, vnitřní IP adresu routeru, IP adresu pro připojení klienta a uživatelské jméno a heslo pro spárování obou zařízení.

The screenshot shows the DD-WRT control panel interface. At the top, there's a status bar with the DD-WRT logo, a progress bar, and system information: "Firmware: DD-WRT v24-sp2 (08/07/10) vpn", "Time: 08:42:51 up 9 min, load average: 0.05, 0.08, 0.07", and "WAN IP: 192.168.123.6". Below this is a navigation menu with tabs: Setup, Wireless, Services (selected), Security, Access Restrictions, NAT / QoS, Administration, and Status. Under the Services tab, there are sub-tabs: Services, VPN (selected), Hotspot, and My Ad Network. The main content area is titled "PPTP Server" and contains a "Help" link and a "more..." link. The PPTP Server configuration section includes the following fields:

- PPTP Server: ☒ Enable ☐ Disable
- Broadcast support: ☒ Enable ☐ Disable
- Force MPPE Encryption: ☒ Enable ☐ Disable
- DNS1:
- DNS2:
- WIN51:
- WIN52:
- Server IP:
- Client IP(s):
- CHAP-Secrets:

Below the PPTP Server section is the "PPTP Client" section, which includes a "PPTP Client" sub-section with the following field:

- PPTP Client Options: ☐ Enable ☒ Disable

**Obr. 25 Nastavení VPN pro server**

Tyto jednoduché kroky nám ukazují jak správně nastavit server pro připojení VPN klienta.

## Nastavení klienta

Nastavení routeru ve statusu klienta bude probíhat obdobně jako u nastavení serveru.

**WAN Setup**

**WAN Connection Type**

Connection Type:

STP: ☐ Enable ☒ Disable

**Optional Settings**

Router Name:

Host Name:

Domain Name:

MTU:

**Network Setup**

**Router IP**

Local IP Address:

Subnet Mask:

Gateway:

Local DNS:

**Network Address Server Settings (DHCP)**

DHCP Type:

DHCP Server: ☒ Enable ☐ Disable

Start IP Address: 192.168.2.

**Help** [more...](#)

**Automatic Configuration - DHCP:**  
This setting is most commonly used by Cable operators.

**Host Name:**  
Enter the host name provided by your ISP.

**Domain Name:**  
Enter the domain name provided by your ISP.

**Local IP Address:**  
This is the address of the router.

**Subnet Mask:**  
This is the subnet mask of the router.

**DHCP Server:**  
Allows the router to manage your IP addresses.

**Start IP Address:**  
The address you would like to start with.

**Maximum DHCP Users:**  
You may limit the number of addresses your router hands out. 0 means only predefined static leases will be handed out.

Obr. 26 Nastavení Basic Setup pro klienta

V kolonce **Advancedrouting** nastavíme veřejnou adresu serveru a síť, na které server pracuje.

dd-wrt.com ... control panel

Firmware: DD-WRT v24-sp2 (08/07/10) vpn  
Time: 08:47:05 up 13 min, load average: 0.18, 0.10, 0.08  
WAN IP: 192.168.123.2

Setup Wireless Services Security Access Restrictions NAT / QoS Administration Status

Basic Setup DDNS MAC Address Clone **Advanced Routing** VLANs Networking EoIP Tunnel

**Advanced Routing** Help more...

**Operating Mode**

Operating Mode

**Static Routing**

Select set number  Delete

Route Name

Metric

Destination LAN NET

Subnet Mask

Gateway

Interface

Show Routing Table

Save Apply Settings Cancel Changes

**Operating Mode:**  
If the router is hosting your Internet connection, select *Gateway* mode. If another router exists on your network, select *Router* mode.

**Select set number:**  
This is the unique route number, you may set up to 50 routes.

**Route Name:**  
Enter the name you would like to assign to this route.

**Destination LAN NET:**  
This is the remote host to which you would like to assign the static route.

**Subnet Mask:**  
Determines the host and the network portion.

Obr. 27 Nastavení Advanced Routing pro klienta



Dále budeme pokračovat s nastavením v Services – VPN – PPT klient. Zde opět nastavíme veřejnou IP adresu serveru, se kterým se chceme spárovat. Dále nastavíme přístupové jméno a heslo pro připojení.

The screenshot shows the Mikrotik WinBox interface with the following configuration details:

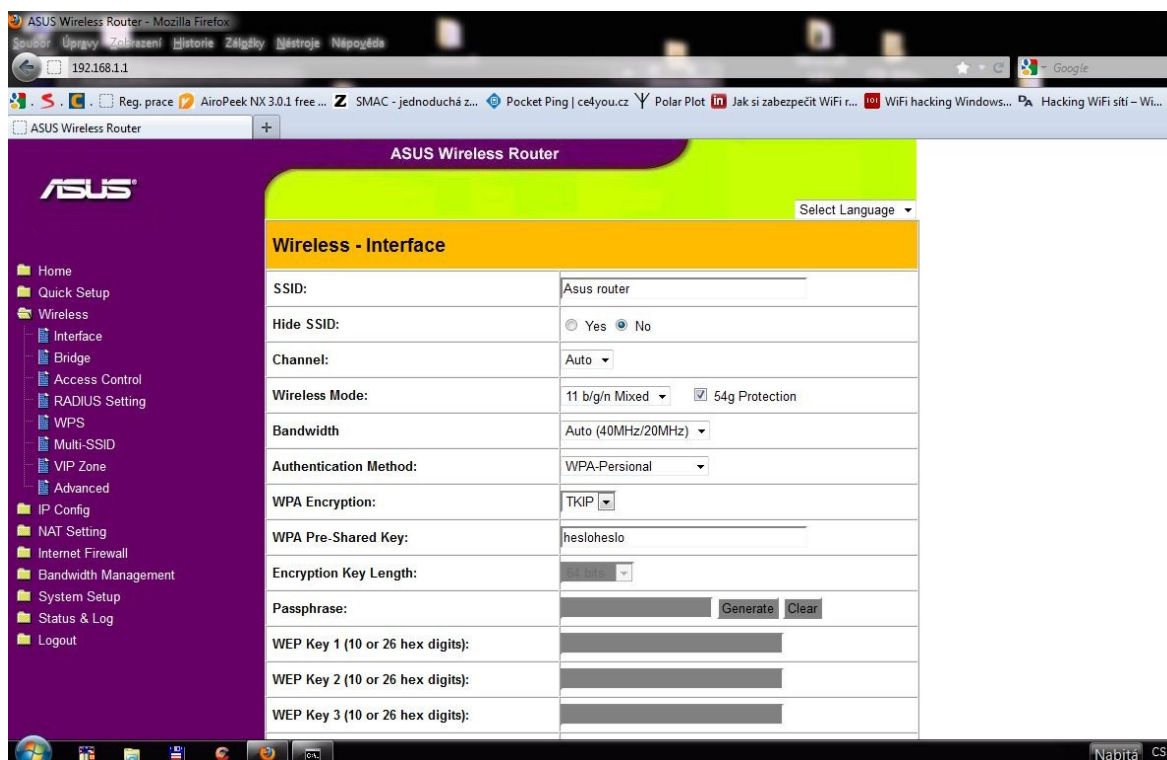
- Services Menu:** Setup, Wireless, **Services**, Security, Access Restrictions, NAT / QoS, Administration, Status.
- VPN Sub-menu:** **Services**, **VPN**, Hotspot, My Ad Network.
- PPTP Server Section:**
  - PPTP Server:** ☐ Enable ☒ Disable
- PPTP Client Section:**
  - PPTP Client:** ☒ Enable ☐ Disable
  - PPTP Client Options:**
    - Server IP or DNS Name: 192.168.123.6
    - Remote Subnet: 192, 168, 1, 0
    - Remote Subnet Mask: 255, 255, 255, 0
    - MPPE Encryption: mppe required
    - MTU: 1450 (Default: 1450)
    - MRU: 1450 (Default: 1450)
    - NAT: ☒ Enable ☐ Disable
    - User Name: user
    - Password: test ☒ Unmask
- OpenVPN Daemon Section:**
  - OpenVPN Daemon:** ☐ Enable ☒ Disable

Obr. 28 Nastavení VPN pro klienta

### 5.3 Realizace správného umístění antény přístroje v prostorách bytu

Tato úloha není nějak složitá, jediné co zde musíme provést, je správně nastavit router a použít vhodné zařízení se správným softwarovým vybavením. Nejvhodnější bude použít dostupné PDA s nástrojem vytvořeným speciálně pro detekci a pingování sítí.

Tým nastaví příslušný router dle známých nastavení tak, aby se do vytvoření WiFi sítě mohli zařízení bez problému připojovat.

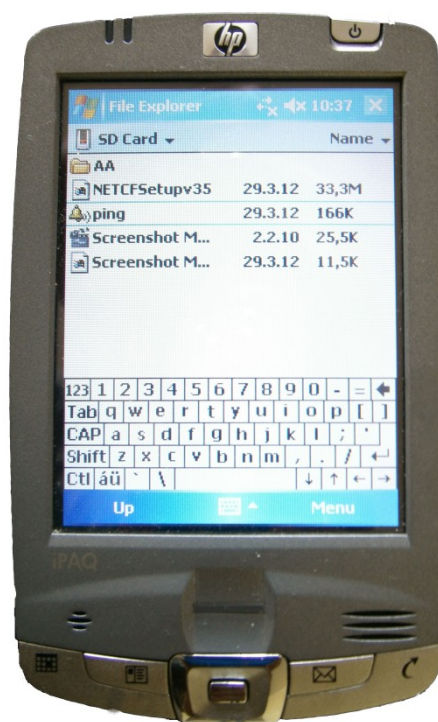


Obr. 29 Nastavení routeru s vhodným zabezpečením

Ping při své činnosti periodicky odesílá IP datagramy a vyčkává na odezvu protistrany. Při úspěšném obdržení odpovědi vypíše délku zpoždění a na závěr vypíše statistický souhrn.

Poté, co dostanou studenti PDA, musí jej patřičně připravit na úkony spojené s úlohou. Studenti ověří, jestli má přístroj plně nabitá baterie, pokud tak nebude, musí přístroj dobít. Poté je potřeba zajistit vhodný software pro práci. Pokud jej studenti

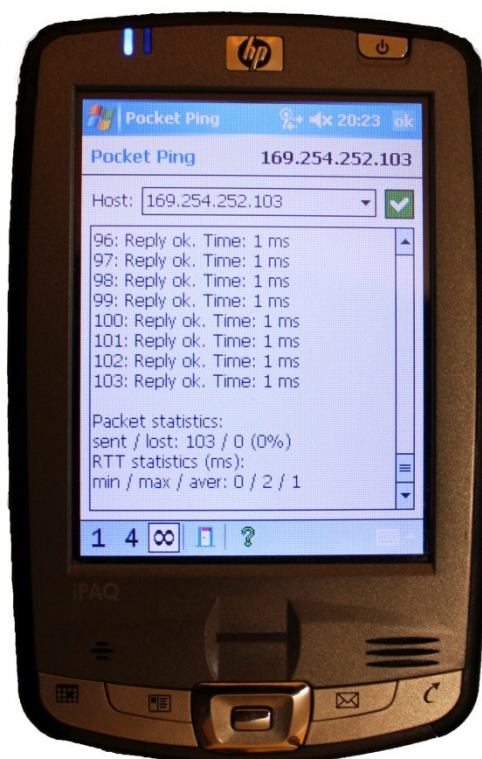
nenajdou přímo v PDA, musí jej najít na internetu a do přístroje nahrát. Toto se provede buďto pomocí kabelu a připojení k PC nebo pomocí nahrání softwaru na Micro SD kartu, která se následně vloží do PDA.



**Obr. 30 Program potřebný pro práci na SD kartě**

Tým se bude pohybovat v daných zónách a budou měřit délku odezvy. Díky získaným poznatkům již budeme vědět kde je pro anténu nejlepší vhodné místo pro umístění.

Nástroj, který je vhodný k použití pro získávání odezvy se jmenuje Pocket Ping. Použili jsme verzi 1.7. Tento softwarový nástroj je freeware, a tudíž je zdarma ke stažení na internetových stránkách.



**Obr. 31 Ukázka použití nástroje Pocket Ping**

## 6 Závěr

Tato bakalářská práce se zabývá technologií WiFi a problematikou výuky této technologie v týmech. Je rozdělena do dvou částí – teoretické a praktické.

Část teoretická se věnuje WiFi technologii jako celku a týmové práci z organizačního pohledu včetně rolí jednotlivců v týmu. V úvodu jsou popsány důvody vzniku bezdrátové technologie WiFi, její základní prvky a principy fungování. Další kapitola se věnuje hardwaru, který je potřebný k vytvoření bezdrátové sítě a také základním principům využití jeho jednotlivých komponent. V posledních teoretických kapitolách se bakalářská práce zaměřuje na problematiku řešení úkolů v týmech a na efektivní způsoby práce se zadanými úlohami.

Jedním z důležitých bodů zadání této práce bylo vytvořit základní týmové úlohy pro studenty na jednu až dvě vyučovací hodiny. Proto jsou v rámci praktické části navrženy tři různé úlohy, které jsou vhodné pro získání poznatků a praktických dovedností potřebných k pochopení správného využívání technologie WiFi. Úkoly jsou zpracovány včetně řešení tak, aby bylo možné na základě praktických pokusů odvodit teoretické znalosti.

Studenti se zde dovědí vše potřebné k pochopení základů WiFi technologií. Postupně přejdou od pochopení teoretické funkčnosti WiFi přes hardwarové a softwarové vybavení až k samotnému řešení různých problémů a úloh. Pro toto řešení je potřeba vždy získat veškeré potřebné informace. Studenti závěrečného ročníku inženýrského studia budou moci pracovat samostatně a bez větší pomoci vyučujícího mohou získat potřebné informace pro různé úkoly zaměřené na WiFi technologii. Vyučující zde nebude hodnotit studenty jako takové, ale bude hodnotit práci, kterou budou schopni vyprodukovat jako tým. Management počítačových sítí je zaměřený na doplnění praktických znalostí, na které do té doby v osnovách studia nezbylo místo. Ve chvíli, kdy tento předmět dojde v časovém harmonogramu k výuce zaměřené na WiFi technologie, se stává vyučující konzultantem a poradcem studentů.

Projekt může být dále rozvíjen vytvořením obdobných úloh, které by studenti zpracovávali pro získání konkrétnějších informací v různých odvětvích WiFi technologie. Jako přílohu přidávám CD s návody do cvičení v elektronické verzi.

Po realizaci uvedených úloh v rámci daného předmětu si studenti uvědomí, jak v praxi probíhá týmová práce. Umožní jim to snadněji navrhovat a realizovat počítačové sítě za různých podmínek.

## 7 Seznam použité literatury

ASPA, a.s. - *Internetový obchod* [online]. [cit. 2012-01-05]. Dostupné z:  
<http://wifi.aspa.cz/>

BARTÁČEK, J. - *Stránky o elektronice a počítačích* [online]. [cit. 2012-01-05]. Dostupné z <http://www.barts.cz/index.php/pocitace/site/29-bezdratovesite>

DD-WRT.COM - *Webový portál se softwarem pro routery*. [online]. [cit. 2012-01-05].  
Dostupné z: <http://dd-wrt.com/site/index>

DOUBLER, J. - *Linuxsoft.cz* [online]. [cit. 2012-01-05]. Dostupné z  
[http://www.linuxsoft.cz/article.php?id\\_article=107](http://www.linuxsoft.cz/article.php?id_article=107)

Extra Publishing, s. r. o. 2007–2011. - *Test routeru* [online]. [cit. 2012-01-05]. Dostupné z:  
<http://extrahardware.cnews.cz/test-routeru-linksys-e3000-poddejte-se-maximu?page=0,2>

FARANA, R., SMUTNÝ, L., VÍTEČEK, A. 1999 - *Zpracování odborných textů z oblasti automatizace a informatiky*. 1. vyd. Ostrava : VŠB-TU Ostrava, 1999. 68 s. ISBN 80-7078-737-6.

KÖHRE, T. - *Stavíme si bezdrátovou síť Wi-Fi*, Praha: ComputerPress 2004. 296 s. ISBN: 80-251-0391-9

MUDROCH, M. - *Stránky katedry elektromagnetického pole* [online]. [cit. 2012-01-05].  
Dostupné z:  
[http://www.elmag.org/doku.php/k317:simulace\\_elmag\\_poli:vyzarovaci\\_diagram](http://www.elmag.org/doku.php/k317:simulace_elmag_poli:vyzarovaci_diagram)

PECHAČ, P. - *Šíření vln v zástavbě*. Praha: BEN - technická literatura 1. vyd. 2005. 108 s. ISBN 80-7300-186-1

PILNÝ, R. – *Teorie o anténách*[online]. [cit. 2012-04-11].

Dostupné z:

<http://www.rc-eagleeye.cz/rc-eagleeye/5-Theory-Trocha-teorie/13-Antennas-Anteny#Line%C3%A1rn%C3%AD%20polarizace>

PUŽMANOVÁ, R. 2005 - *Bezpečnost bezdrátové komunikace*. 1. vyd. Brno: Computerpress, 2005. 179 s. ISBN 80-251-0791-4.

ZANDL, P. - *Bezdrátové sítě WiFi – Praktický průvodce*. 1. vyd. Brno: Computerpress, 2003. 190 s. ISBN 80-7226-632-2.



## **Seznam příloh**

Přílohy obsahují CD

CD obsahuje:

I. Elektronické vydání bakalářské práce

II. Podpůrné materiály k vytvořeným úlohám